broadband forum

TECHNICAL REPORT

TR-177
IPv6 in the context of TR-101

Issue: 1
Issue Date: November 2010

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Broadband Forum Technical Report has been approved by members of the Forum. This Broadband Forum Technical Report is not binding on the Broadband Forum, any of its members, or any developer or service provider. This Broadband Forum Technical Report is subject to change, but only with approval of members of the Forum. This Technical Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be copyrighted by Broadband Forum members.

This Broadband Forum Technical Report is provided AS IS, WITH ALL FAULTS. ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY:

(A) OF ACCURACY, COMPLETENESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE;
(B) THAT THE CONTENTS OF THIS BROADBAND FORUM TECHNICAL REPORT ARE SUITABLE FOR ANY PURPOSE, EVEN IF THAT PURPOSE IS KNOWN TO THE COPYRIGHT HOLDER;
(C) THAT THE IMPLEMENTATION OF THE CONTENTS OF THE TECHNICAL REPORT WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

By using this Broadband Forum Technical Report, users acknowledge that implementation may require licenses to patents. The Broadband Forum encourages but does not require its members to identify such patents. For a list of declarations made by Broadband Forum member companies, please see http://www.broadband-forum.org. No assurance is given that licenses to patents necessary to implement this Technical Report will be available for license at all or on reasonable and non-discriminatory terms.

ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW (A) ANY LIABILITY (INCLUDING DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES UNDER ANY LEGAL THEORY) ARISING FROM OR RELATED TO THE USE OF OR RELIANCE UPON THIS TECHNICAL REPORT; AND (B) ANY OBLIGATION TO UPDATE OR CORRECT THIS TECHNICAL REPORT.

Broadband Forum Technical Reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only, and may not be modified without the advance written permission of the Broadband Forum.

The text of this notice must be included in all copies of this Broadband Forum Technical Report.

Issue History

Issue Number	Issue Date	Issue Editor	Changes
1	November 2010	Sven Ooghe, Alcatel-Lucent Bala'zs Varga, Ericsson Wojciech Dec, Cisco Systems	Original

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.

Editors	Sven Ooghe Bala'zs Varga Wojciech Dec	Alcatel-Lucent Ericsson Cisco Systems
E2E Architecture WG Chairs	David Allan David Thorne	Ericsson BT
Vice Chair	Sven Ooghe	Alcatel-Lucent
Chief Editor	Michael Hanrahan	Huawei Technologies

Table of Contents

List of Figures

Executive Summary

TR-177 documents modifications to the TR-101 architecture to permit dual stack IPv4 and IPv6 operation. As such TR-177 extends the TR-101 architecture to add IPv6 based services and applications to the suite of services already supported by TR-101. This Technical Report presents the requirements for protocol interworking and security for the network elements that are part the TR-101 architecture.

Using the IPv6 connectivity described in TR-177, Service Providers will be able to provide basic IPv6 services like tiered Internet access. Initial IPv6 deployments are expected to be done for unicast services, with multicast services like IPTV as a future step. The current version of TR-177 describes this first step, including a description of the IPv6 multicast functions that are necessary to support IPv6 unicast connectivity. It also outlines the second step, but without describing the deployment scenario and corresponding requirements in detail.

1 Purpose and Scope

1.1 Purpose

Since the introduction of the World-Wide Web (WWW), the Internet has witnessed a remarkable growth. This success has lead to a continuing demand for Internet Protocol (IP) network addresses. As a result of this, continued deployment of the current version of the Internet Protocol – IPv4 – is very likely to encounter constraints in the coming years; for which the exhaustion of the pool of unallocated IPv4 addresses is commonly considered as the key constraint.

Recent studies reveal that - given the current trend of address consumption - the unallocated IPv4 address pool will be exhausted very soon. A very good study can be found on http://www.potaroo.net/tools/ipv4/, which predicts IPv4 address exhaustion at the IANA level by the second half of 2011. The report mentions that there is an opportunity to prolong the life of IPv4 by bringing the allocated, but unadvertised IPv4 addresses back into play (e.g. by introducing new pricing policies that stimulate users to efficiently use their allocated addresses). In this case, predictions suggest that some further growth of IPv4 deployment could continue.

The increasing demand for IP addresses, together with a number of other design issues, triggered the development of an upgrade of IPv4, now known as IPv6. One of the main challenges for operators is how to provide connectivity to IPv6 services without impacting existing IPv4-based services and applications.

TR-177 presents a Broadband Forum access network architecture that enables operators to support IPv6. It is built upon Broadband Forum TR-101, which describes a popular and successful Broadband Forum architecture for supporting Ethernet-based DSL aggregation. This Technical Report extends the TR-101 architecture in order to allow the delivery of native Ethernet encapsulated IPv6 and IPv4 packet services. In doing so, it presents the requirements for protocol interworking and security for the network elements that are part the TR-101 architecture: the Residential Gateway, Access Node and Broadband Network Gateway.

1.2 Scope

TR-177 outlines how a TR-101 [1] network architecture can be enhanced to support Ethernet encapsulated IPv6 services in conjuction with IPv4 packet services. The requirements spelled out in this Technical Report equally apply to a GPON access network architecture, as defined in TR-156 [2].

TR-177 builds on the Residential Gateway, Access Node, Aggregation Node and Broadband Network Gateway requirements defined in Broadband Forum TR-101, as components of the architecture. Therefore, a considerable part of the network architecture remains untouched.

The following aspects are described in TR-177:

- Operation of IPv6oE across the access network

- IPv6 deployment models, including placing IPv4 and IPv6 traffic into different VLANs on the V interface (based on the Ethertype)
- Dual stack operation in the access network – with related Residential Gateway (RG), Access node and Broadband Network Gateway (BNG) requirements
- IPv6oE addressing models
- 1:1 VLAN
  - Access Line characterization
  - Security methods and their impact on IPv6 address assignment
- N:1 VLAN
  - Access Line identification and characterization
  - L2 Security (ICMPv6 / ND / DAD, DHCPv6)

The following aspects remain unchanged from TR-101:

- The supported physical interfaces across the U and V reference points
- Access Node deployment options
- IPv4 services (IPv4oE, IPv4oA)
- All Ethernet-related architecture and network element requirements, including:
  - VLAN handling, except for protocol-based VLAN assignment
  - Ethernet QoS mechanisms
  - Ethernet OAM mechanisms (IEEE 802.1ag)
- All Ethernet Aggegation Node requirements
- All PPP-related interworking functions, including:
  - PPPoE Intermediate Function
  - PPPoA to PPPoE interworking: regardless of whether the RG uses PPPoE or PPPoA, the PPP phases are identical, so there's no impact on the IPv6 connectivity establishment (see also RFC 5072 [8] and RFC 5172 [9])
- Business services support
- Policy management

The following aspects are out of scope:

- any BNG requirements that are related to the delineation or metering and establishment of the IPv6 subscriber sessions – will be described in a future Broadband Forum Technical Report. It is currently being developed in Broadband Forum WT-146 *Subscriber Sessions*, which is a work-in-progress.
- The operation of IPv6 over ATM using routed encapsulation across the U reference point: it is assumed that new IPv6 services will be supported over ATM using bridged encapsulation per RFC 2684 [10]
- The operation of PPPv6 over ATM – this is defined in TR-187 [4]
- Any IPv6 transitional technology, e.g. softwire based mechanisms, NAT44, NAT64. In particular, this Technical Report does not consider the case of a host that is only allocated an IPv6 address and requires access to an IPv4 service
- The migration mechanisms across the A10-NSP or A10-ASP reference points (e.g. IPv6 over IPv4 tunneling, 6PE)

Current deployments of unicast and multicast services are based on IPv4. Initial IPv6 deployments are expected to be done for unicast services, with multicast services as a future step.

The current version of the Technical Report describes this first step, including a description of the IPv6 multicast functions that are necessary to support IPv6 unicast connectivity. It also outlines the second step, but without describing the deployment scenario and corresponding requirements in detail.

TR-177 does not provide details/requirements with respect to scale and performance of individual elements, but rather focuses on documenting a functional architecture and the requirements necessary to support it.

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119.

MUST	This word, or the term “REQUIRED”, means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective “RECOMMENDED”, means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the adjective “OPTIONAL”, means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.
A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

[1] Broadband Forum TR-101 (May 2006), Migration to Ethernet-Based DSL Aggregation
[2] Broadband Forum TR-156 Issue 2 (September 2010), Using GPON Access in the context of TR-101
[3] Broadband Forum TR-124 Issue 2 (May 2010), Functional Requirements for Broadband Residential Gateway Devices
[4] Broadband Forum TR-187 (April 2010), Migration to IPv6 using PPP
[5] IETF RFC 2460, Internet Protocol, Version 6 (IPv6)

[6] IETF RFC 2463, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
[7] IETF RFC 4291, IP Version 6 Addressing Architecture
[8] IETF RFC 5072, IP Version 6 over PPP
[9] IETF RFC 5172, Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol
[10] IETF RFC 2684, Multiprotocol Encapsulation over ATM Adaptation Layer 5
[11] IETF RFC 2464, Transmission of IPv6 Packets over Ethernet Networks
[12] IETF RFC 4861, Neighbor Discovery for IPv6
[13] IETF RFC 4862, IPv6 Stateless Address Autoconfiguration
[14] IETF RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
[15] IETF RFC 3633, IPv6 Prefix Options for DHCPv6
[16] IETF RFC 4649, DHCPv6 Relay Agent Remote-ID Option
[17] IETF RFC 5460, DHCPv6 Bulk Leasequery
[18] IETF RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers
[19] IETF RFC 3162, RADIUS and IPv6
[20] IETF RFC 2710 Multicast Listener Discovery (MLD) for IPv6
[21] IETF RFC 3810 Multicast Listener Discovery 2 (MLDv2) for IPv6
[22] IETF RFC 4294, IPv6 Node Requirements
[23] IETF RFC 4601, Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)
[24] IETF draft-ietf-dhc-dhcpv6-ldra, "Lightweight DHCPv6 Relay Agent", Work in Progress
[25] IETF draft-krishnan-6man-rs-mark, "Line identification in IPv6 Router Solicitation messages", Work in Progress
[26] IETF draft-gundavelli-v6ops-l2-unicast, "Unicast Transmission of IPv6 Multicast Messages on Link- layer", Work in Progress
[27] IETF draft-ietf-dhc-dhcpv6-agentopt-delegate, "DHCPv6 Relay Agent Assignment Notification (RAAN) Option", Work in Progress
[28] IETF draft-ietf-radext-ipv6-access, "RADIUS attributes for IPv6 Access Networks", Work in Progress
[29] IETF draft-costa-6man-dad-proxy, "Duplicate Address Detection Proxy", Work in Progress

2.3 Definitions

The following terminology is used throughout this Technical Report.

Access Loop	The physical connectivity between the NID, at the customer premises, and the Access Node.
Access Network	The Access Network encompasses the elements of the network from the Network Interface Device (NID) at the customer premises to a Broadband Network Gateway. This network typically includes one or more types of Access Node and may include an Ethernet aggregation function.

Access Node (AN)	The Access Node terminates the phyiscal layer (e.g. DSL xTU-C function or GPON termination function), may physically aggregate other nodes implementing such functionality, or may perform both functions at the same time. In the scope of this specification, this node contains at least one standard Ethernet interface that serves as its northbound interface into which it aggregates traffic from several user ports or Ethernet-based southbound interfaces.
Broadband Network Gateway (BNG)	IP Edge Router where bandwidth and QoS policies may be applied.
link-local address	An address having link-only scope that can be used to reach neighboring nodes attached to the same link. All interfaces have a link-local unicast address.
solicited-node multicast address	A multicast address to which Neighbor Solicitation messages are sent. The algorithm for computing the address is given in RFC 4291.
Numbered WAN model	The WAN interface of the RG has its own IPv6 GUA.
Unnumbered WAN model	The WAN interface of the RG does not have its own IPv6 GUA.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

AAA	Authentication, Authorization and Accounting
AN	Access Node
BNG	Broadband Network Gateway
BRAS	Broadband Remote Access Server
DHCP	Dynamic Host Configuration Protocol
DAD	Duplicate Address Detection
DSL	Digital Subscriber Line
GUA	Globally-unique Unicast Address
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPoE	IP over Ethernet
IWF	Interworking Function
MAC	Media Access Control
MLD	Multicast Listener Discovery
NA	Neighbor Advertisement

ND	Neighbor Discovery
NS	Neighbor Solicitation
NID	Network Interface Device
NUD	Neighbor Unreachability Detection
PPP	Point to Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
QoS	Quality of Service
RADIUS	Remote Access Dial In User Services
RA	Router Advertisement
RG	Residential Gateway
RS	Router Solicitation
SLAAC	Stateless Address Auto Configuration
TR	Technical Report
ULA	Unique Local Address
VLAN	Virtual LAN
WG	Working Group
WT	Working Text

2.5 Relation to other documents

TR-187 [4] presents the RG and BNG requirements to enable operators to provide IPv6 connectivity in conjunction with IPv4 without impacting the presently deployed access and aggregation network. It is based upon Broadband Forum TR-059 and TR-101, specifying a PPP-based connectivity scheme between the RG / Home Network and the BNG. The document specifies the IPv6 connectivity and addressing aspects to enable IPv6-based services and applications by means of PPP.

The Broadband Forum is working on a document (WT-146, *Subscriber Sessions*) that presents a description of the concepts of an IPv4 and IPv6 session and IP Session grouping for deployment in a TR-101 based architecture. The document re-uses architectural notions introduced in TR-59 and TR-101 architectures, and places requirements on the Residential Gateway (RG) and IP Edge (i.e. the BNG) devices to establish and maintain single (IPv4 or IPv6) or dual stack (IPv4/IPv6) sessions. Note: This is a work-in-progress and as such is a Broadband Forum internal document only available to members of the Broadband Forum.

3 Technical Report Impact

3.1 Energy Efficiency

The addition of IPv6 traffic handling in the access network is not expected to create any significant increase in energy expenditure compared to the equivalent PPP and IPv4 based traffic handling.

3.2 IPv6

TR-177 leverages existing RFCs for IPv6 capabilities. No extensions of IPv6 protocols are defined in this Technical Report. TR-177 also references draft-ietf-dhc-dhcpv6-ldra, draft-ietf-dhc-dhcpv6-agentopt-delegate, draft-ietf-radext-ipv6-access, draft-krishnan-6man-rs-mark, draft-gundavelli-v6ops-l2-unicast and draft-costa-6man-dad-proxy as work in progress. This work may result in additional IANA allocations.

3.3 Security

TR-177 introduces a number of IPv6 specific security requirements, which are based on the equivalent IPv4 security requirements defined in TR-101.

4 Fundamental Architectural and Topological Aspects

4.1 IPv6 deployment models

This Technical Report describes the support of IPv6 according to a "dual stack" approach, i.e. supporting both IPv4 and IPv6 concurrently within the access network. This implies that the network nodes support IPv4 and IPv6 sessions independently. Dual stack hosts can support IPv4 and IPv6, however this does not imply they always require both IPv4 and IPv6 connectivity.

The overall architecture is based on the architecture defined in Section 2/TR-101, and in particular on the model shown in Figure 3/TR-101.

The architecture builds on TR-101 1:1 VLAN and N:1 VLAN models. As a result, the requirements related to a number of encapsulations across the U reference point can be applied without change:

- IPv4 over Ethernet related requirements
- IPv4 over ATM (routed encapsulation) related requirements
- PPPoE Intermediate Agent related requirements: the Access Node processes the PPPoE header, without looking at the actual PPP payload. As a result the PPPoE Intermediate Agent requirements remain unchanges when supporting IPv6 over PPPoE
- PPPoA to PPPoE interworking function: the Access Node processes the PPP LCP packets, but does not need to look at the IPCP or IPv6CP packets (see also RFC 5072 [8] and RFC 5172 [9]). As a result, the PPPoA to PPPoE interworking requirements remain unchanged when supporting IPv6 over PPPoA

The requirements in TR-177 are primarily focusing on the support of IPv6 over Ethernet encapsulation (RFC 2464 [11]) across the U and V reference point. In doing so, extensions to TR-101 are defined when required to support IPv6.

This Technical Report specifies support for IPv6 over ATM using bridged encapsulation per RFC 2684 [10]. In order to simplify the interworking with Ethernet uplinks, the operation of IPv6 over ATM using routed encapsulation across the U reference point is not recommended and is therefore out of the scope of this Technical Report.

4.2 IPv6 addressing recommendations

There are three types of IPv6 addresses: unicast, anycast and multicast (see RFC 4291 [7]). Unicast IPv6 addresses of these types are assigned to interfaces, not nodes.

IPv6 nodes need one or more unique IPv6 unicast addresses to be able to communicate. Unicast IPv6 address types are as follows: (i) link-local address, (ii) Unique Local Address (ULA) and (iii) Globally-unique Unicast Address (GUA).

Different methods can be used for IPv6 address assignment to an interface. Addresses can be generated:

- manually
- via stateless address autoconfiguration (SLAAC, RFC 4862 [13])
- via stateful DHCPv6 (RFC 3315 [14]) or DHCPv6-PD (RFC 3633 [15])

Section 4.2/TR-187 specifies that the Broadband Forum architecture does not use the DHCPv6 Temporary Address (IA_TA option). This remains applicable to TR-177..

The main focus of TR-177 is on following scenarios:
- a subscriber having a routed RG. This RG can be connected to the access loop either directly or through a bridged RG. The routed RG acts as a Requesting Router (as per RFC 3633), and possibly embeds DHCPv6-based address allocation capabilities.
- a subscriber having a bridged RG, in which case the first hop router for their hosts is the BNG. The subscriber hosts support DHCPv6 address allocation capabilities.

In all cases SLAAC is supported to obtain link-local addresses and perform Duplicate Address Detection (DAD).

TR-177 presents a description of how SLAAC can be used for global address assignment with N:1 VLANs and bridged RGs, but note that this work depends on IETF drafts that are still work in progress.

In addition to unicast (anycast) addresses, the all-nodes multicast address (ff02::1) and the solicited-node multicast address are required for Neighbor Discovery and therefore fundamental for the functioning of IPv6.The solicited-node multicast address(es) of an interface are derived from the unicast address(es) of that interface and are used when performing address resolution and when testing address uniqueness using DAD.

From a routed RG perspective, the following IPv6 addresses may be provided by the Service Provider's network:

- A /64 prefix for the WAN link GUA (optional, only done in the case of the numbered WAN model)
- A delegated prefix for use within the home network (mandatory). The Broadband Forum suggests a size for the delegated prefix of at least a /60 for home network or SOHO environments, with a recommended prefix length of /56. The delegated prefix may be extended to a /48 for larger organizations.

Best practice for a single subscriber / access line is to use a single global IPv6 prefix for all services on that subscriber / access line.

4.2.1 IPv6 Prefix Delegation (DHCPv6-PD)

The Prefix Delegation options defined in RFC 3633 [15] provide a mechanism for automated delegation of IPv6 prefixes using the Dynamic Host Configuration Protocol (DHCPv6). This mechanism is intended for delegating a prefix from a Delegating Router (DR) to a Requesting Router (RR), across an administrative boundary, where the Delegating Router does not require knowledge about the complete topology of the links in the network. In the case of PD, the routed

RG acts as the Requesting Router and the BNG acts as the Delegating Router. Note also that the use of PD also implies that hosts receiving IPv6 addresses from the RR are not known to the BNG, i.e. the BNG is not aware of what addresses/prefixes are assigned to hosts attached to the RG acting as RR.

A different prefix (with a maximum length of 64 bits, and a recommended length of 56 bits) is delegated per access loop. This delegated prefix is then distributed as /64 prefixes to the different LAN segments attached to the routed RG. The delegated prefix is therefore never shared across different access loops. This is shown in Figure 1.

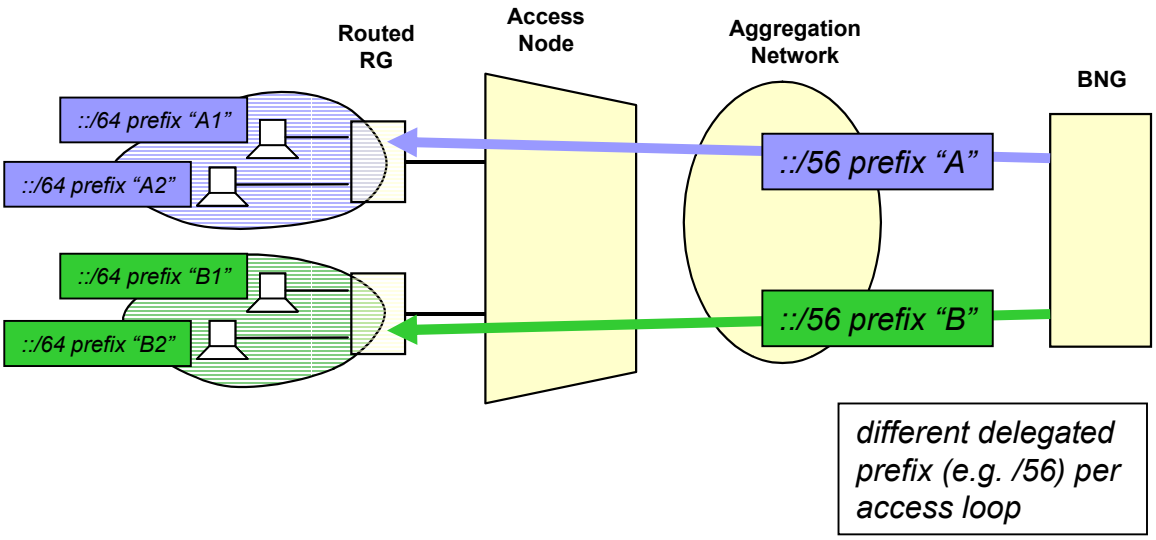

Figure 1 – Address assignment using IPv6 prefix delegation to a routed RG

4.2.2 DHCPv6 address assignment

The DHCPv6 protocol, defined in RFC 3315 [14], can be used to provide a device with both an IPv6 address, assigned by a DHCPv6 server, and other configuration information, which is carried in specific options.

The DHCPv6 server selects 128-bit addresses to be assigned according to the address assignment policies determined by the server administrator and the specific information the server determines about the client from some combination of the following sources:

- The link to which the client is attached
- The DHCP Unique Identifier (DUID) supplied by the client
- Other information in options supplied by the client
- Other information in options supplied by the (lightweight) relay agent (e.g. Option 18 added by the Lightweight DHCPv6 Relay Agent in the Access Node)

In principle, the DHCPv6 server may assign 128-bit addresses to hosts without any correlation between the different addresses. In other words, multiple hosts connected to different access loops could potentially share the same /64 prefix.

The architecture defined in TR-177 provides an addressing/prefixing scheme where /64 prefixes are never shared across access loops. Such a scheme supports both bridged and routed RGs and is independent the type of VLAN model (1:1 or N:1 VLAN).

Therefore, when assigning an IPv6 address to a host, it is recommended that the DHCPv6 Server assigns a different 64-bit prefix per access loop or per host, depending on Service Provider's choice. In all cases, the first 64-bit prefix of the assigned IPv6 address must never be shared between DHCPv6 clients connected to different access loops.

If DHCPv6 is used to assign a /128 IPv6 address to the RG WAN interface (for management of the RG), the BNG can use the same /64 for different RGs

4.2.3 StateLess Address AutoConfiguration (SLAAC)

The IPv6 Stateless Address AutoConfiguration mechanism (RFC 4862 [13]) allows a host to generate its own addresses using a combination of locally available information and information advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an “interface identifier” that uniquely identifies an interface on a subnet. An address is formed by combining the two pieces of information. Currently many commercially available IPv6 hosts use SLAAC for address assignment.

In the absence of routers, a host can only generate link-local addresses which are limited in their use to communication between nodes attached to the same link.

The prefix information is sent to the host using the Prefix Information Option (PIO) which is part of the Router Advertisement (RA) message. A different /64 prefix is advertised per access loop or per host, depending on Service Provider’s choice; a 64-bit prefix is never shared across different access loops. This is shown in Figure 2.

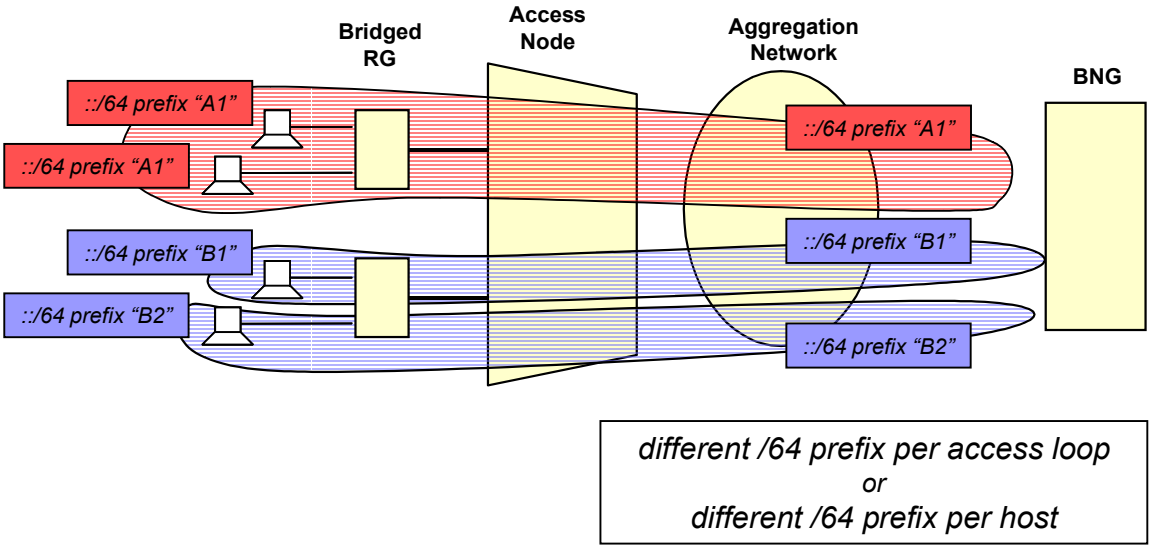

Figure 2 – Address assignment using SLAAC to hosts connected to a bridged RG

In a 1:1 VLAN scenario, performing SLAAC-based address assignment does not impact the Access Node or aggregation switches. In this case, the RS message can be used to trigger AAA on the BNG.

4.2.4 Mixed deployment of bridged and routed RGs

Figure 3 shows a network deployment with a mixture of bridged and routed RGs. As can be seen, the /64 prefixes are not shared across access loops, independently of the type of RG used. In the case of a numbered WAN model, an additional subnet per routed RG needs to be allocated (not shown here). Note also that the RG may support a combination of bridged and routed behavior.

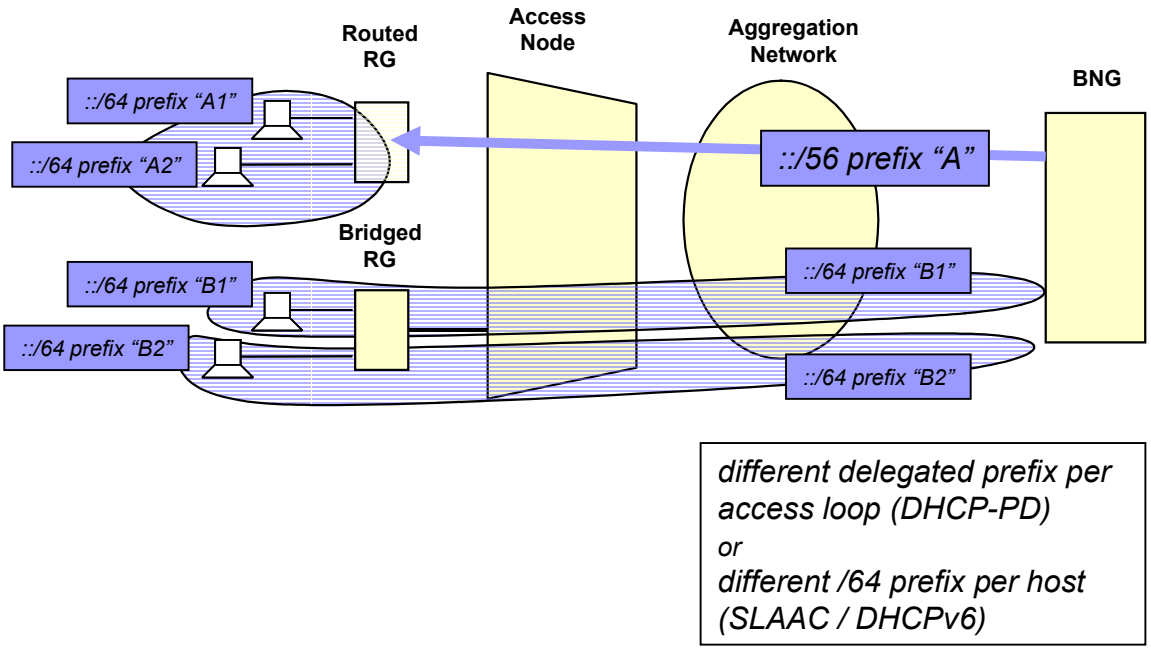

Figure 3 – Address assignment in a mixed deployment of bridged and routed RGs

4.3 Residential Gateway Requirements

The RG requirements to support IPv6 are captured in TR-124 [3].

R-01 The RG MUST be able to retransmit RS messages until it has received an RA message, e.g. by setting MAX_RTR_SOLICITATIONS (Section 10/RFC 4862 [13]) to infinite and using the retransmission algorithm specified for retransmitting SOLICIT messages in DHCPv6 (RFC 3315).

4.4 The U reference point

Figure 4 repeats the (IPv4) protocol stacks at the U reference point, defined in TR-101. Figure 5 shows the IPv6 protocol stacks at the U reference point covered by TR-177, and compares them with their TR-101 counterparts.

PPP-based protocol encapsulations – corresponding to TR-101 options 'b', 'd' and 'f' are defined in TR-187.

Option 'g' does not require the Access Node to have visibility of the network layer protocols. Therefore the Access Node functionality to cover this protocol stack is already defined in TR-101.

This Technical Report does not cover option 'c', i.e. IPv6 over ATM routed encapsulation.

Option ‘a‘ is denoted IPoEoATM. Option ‘e’ represents the scenario when the access loop supports direct Ethernet encapsulation and is referred to as IPoE. Within this Technical Report both options ‘a’ and ‘e’ are commonly referred to as IPoE. A port using IPoE access is generally denoted a bridged port.

Note that the protocol stack may also include 802.1Q headers to carry VLAN tags and/or priority markings.

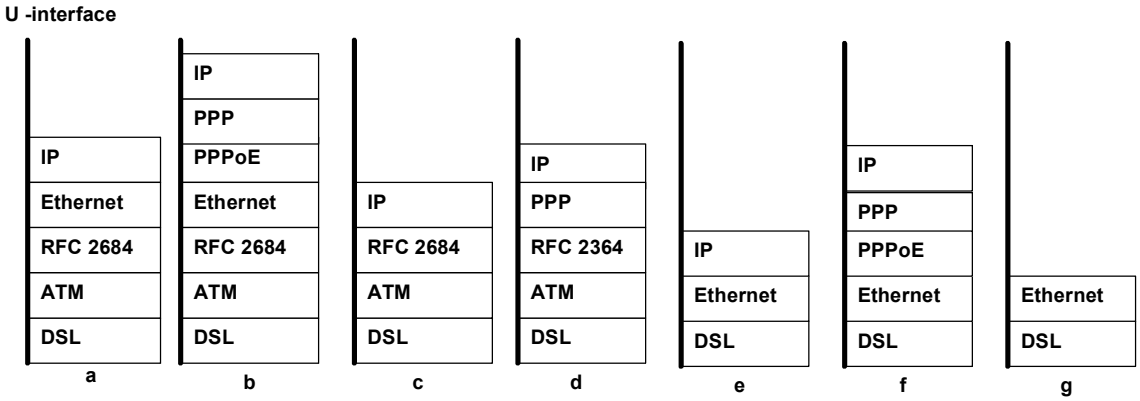

Figure 4 – IPv4 Protocol stacks at the U reference point (TR-101)

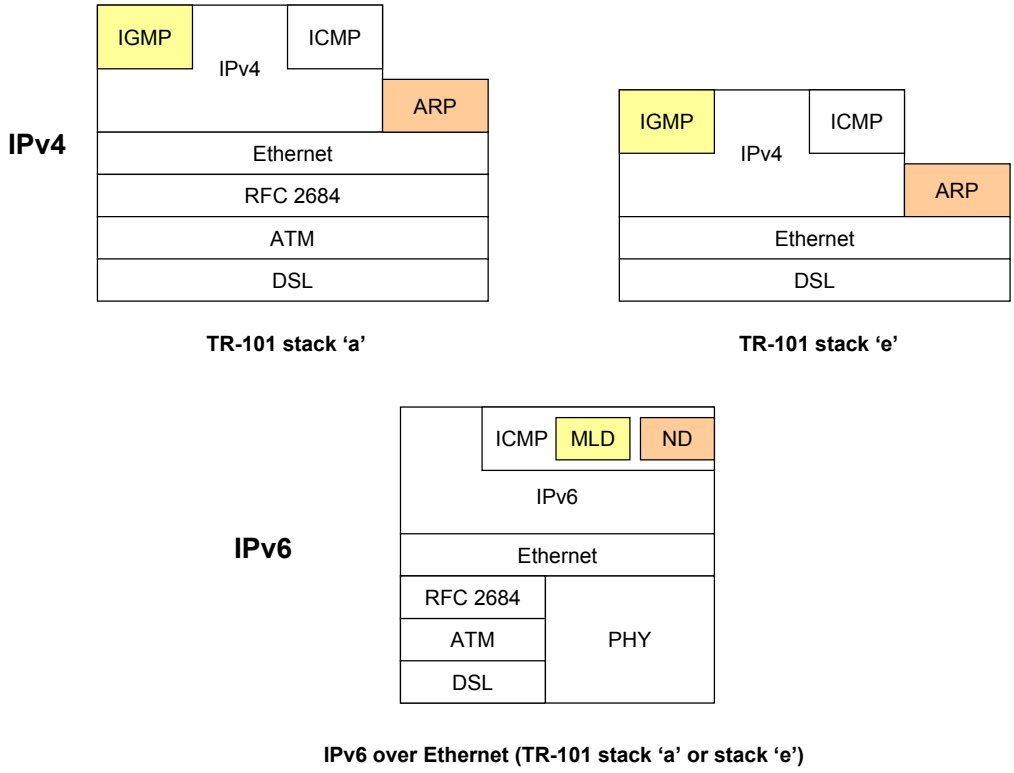

Figure 5 – IPv6 protocol stacks at the U reference point

Figure 5 also shows that in IPv4, ARP uses an Ethertype that is different from that of IPv4. In IPv6, ARP functionality is embedded in ICMPv6. Similarly, in IPv4, IGMP is a dedicated protocol on top of the IPv4 stack, whereas in IPv6, MLD is part of ICMPv6.

The physical layer at the U interface is expected to support different PHY technologies

4.5 Access Node

In addition to the the requirements defined in TR-101/TR-156, the Access Node has to provide an interworking function (IWF) between the U and V reference point, encompassing IPv6-related protocol interworking, access loop identification, QoS and security.

4.6 Broadband Network Gateway

The BNG needs to support a number of IPv6-specific requirements in order to provide the IPv6 connectivity establishment and address assignment. These are covered in Section 6.

Additional BNG requirements related to the handling of IPv6 Sessions will be described in Broadband Forum WT-146, *Subscriber Sessions*.

It is expected that the BNG support dual-stack on the network-facing side, i.e. toward the A10-NSP or A10-ASP reference points. Additional requirements to support IPv6 tunneling or address translation across the A10-NSP or A10-ASP reference points are beyond the scope of TR-177.

4.7 IPv6 Multicast support

IPv6 uses well-known and transient multicast addresses during interface configuration. Well-known multicast addresses in IPv6 are assigned by IANA just as for IPv4. (Thus, an IP packet with a destination address ff02:1:2 is addressed to a DHCP relay, and ff02::16 to an MLD router.). For the many multicast addresses identified below, registering the solicited node address of a host requires the sending of an MLD join or leave to the BNG. In IPv6, MLD is a sub-protocol of ICMPv6 and encapsulation, forwarding for ICMPv6 applies to MLD (see Section 5.6.2).

As per RFC 4294 [22] and RFC 4861 [12], a host or RG behaving as a host on its WAN interface is required to recognize that it is associated with several addresses, some of which are multicast addresses RFC 4291 [7]:

- All-nodes multicast address

  Identifies the group of all IPv6 nodes that are link-local (ff02:0:0:0:0:0:0:1). Link-local addresses include the same group of nodes (RG, BNG). With split horizon forwarding, upstream packets are only forwarded to the BNG. Downstream forwarding behavior is described in Section 5.6.2.

- Solicited-node multicast address

  This multicast address is computed by taking the low-order 24 bits of an address and appending them to the solicited node prefix (ff02:0:0:0:0:1:ff/104) to get an address ff02:0:0:0:0:1:ffX:XXXX. It is possible that more than one IPv6 node belongs to this group. With split horizon forwarding, upstream packets are only forwarded to the BNG. For downstream forwarding behavior of ICMPv6 messages, see Section 5.6.2.

  An RG/host joins or leaves the solicited node address by sending a MLD Multicast Listener Report to the BNG (MLD Querier).

- In TR-177, the host or RG is not required to join any other multicast group (since IP multicast services are maintained at IPv4)

As per RFC 4294 [22] and RFC 4861 [12], a BNG and routed RG behaving as a router (LAN interface) are required to recognize all the host addresses, including the following addresses:

- Subnet router anycast address

  This address is required for a BNG and routed RG (LAN interface). It is constructed by the subnet prefix followed by trailing zeros. Packets sent on the subnet-router anycast address will be delivered to one router on the subnet.

- All-routers multicast address

  Identifies the group of all IPv6 routers on that link (ff02:0:0:0:0:0:0:2).

This version of the Technical Report does not describe IPv6 multicast requirements for the support of IPv6 multicast services such as IPTV. It is expected that initial IPv6-based triple play deployments will maintain the current IPv4-based multicast network architecture. To make this possible, an additional requirement is specified in Section 7.

A description of IPv6 multicast requirements will be the subject of a future version of this Technical Report.

4.8 IPv6 security considerations

4.8.1 Link-local address handling

4.8.1.1 Creation of link-local addresses

In order to enable IPv6 connectivity, every host must first create a link-local address (of the range fe80::/64) in order to allow communication on a single link. The procedure for creating link-local addresses is defined in RFC 4862 [13]. When an IPv6 interface becomes active it will first concatenate its Interface ID with the link-local prefix fe08::/64.

The Interface ID for an Ethernet interface can be derived from the EUI-64 identifier as specified in RFC 2464 [11]. This 64-bit identifier is derived from the 48-bit interface MAC address.

For example: an interface MAC address 00-1B-E9-58-B0-6D would be mapped to a 64-bit Interface ID 02-1B-E9-FF-FE-58-B0-6D. As a result, the link-local address would be fe80::21b:e9ff:fe58:b06d.

To protect against cases where the Interface ID would not be unique, IPv6 nodes test their address on the IPv6 link using Duplicate Address Detection (DAD). This test is performed to ensure uniqueness of the link-local address on the link.

4.8.1.2 Ensuring link-local address uniqueness in the access network

The above procedures work well in a trusted environment, however a broadband access network is generally an untrusted network because:

- a malicious user may try to spoof a link-local address (e.g. by connecting a PC to a bridged modem and configuring a specific link-local address on the PC)
- a malicious user may try to flood the network with a large number of different link-local addresses, leading to a Denial of Service attack on the BNG

In addition to this, user-to-user communication is controlled in a broadband access network by means of split horizon forwarding, as per TR-101. As a result, link-local communication is only possible between the routed RG or – in the case of an N:1 VLAN model – hosts behind a bridged RG, and the BNG. There is no way for the different routed RG WAN interfaces or hosts behind a bridged RG to know if they are using duplicate link-local addresses.

Finally, in the case where two devices happen to have the same Ethernet MAC address, the link-local address derived for that interface will also be non-unique, provided it is derived from the EUI-64 identifier.

The BNG normally has no way of ensuring that duplicate link-local addresses are handled correctly. It can at best support a “first come first served” behavior and signal to the hosts/RGs when a duplicate link-local address exists.

4.8.1.3 Solutions

In case a routed RG is deployed that complies to TR-124 [3], the MAC address of the RG WAN interface will be unique. As a result, the derived link-local address will also be unique, so duplicate link-local addresses won’t occur.

On the other hand, in case an IPv6 node is used that does not have a guaranteed unique MAC address, or in case of a malicious user, the link-local address may not be unique. In such a case, one solution is to implement a Duplicate Address Detection (DAD) Proxy function on the BNG. The basic principles of such a Proxy are described in Annex B.

5 Access Node Requirements

This section provides a set of requirements to support the architecture defined in Section 4. Unless stated otherwise, the Access Node requirements presented in TR-101 remain applicable. These requirements are now extended with IPv6 specific requirements.

5.1 VLANs

The following addresses the case where a combination of multiple bridged encapsulations – IPv4oE, IPv6oE and PPPoE – are multiplexed over a single user port, but require different VLAN ID and/or priority assignment. The following describes a basic classification mechanism only applicable for untagged and priority-tagged frames (and thus for ports configured to receive those types).

R-02 The Access Node MUST be able to assign an Ethertype filter to a given port.

At least the following types MUST be supported

- IPv6oE (Ethertype = 0x86DD) – note: ICMPv6 is identified by a Next Header value of 58 in the immediately preceding IPv6 header
- PPPoE (Ethertype = 0x8863 and 0x8864)
- IPv4oE (Ethertype = 0x0800)
- ARP (Ethertype = 0x0806)

Note that this is an augmentation of R-26/TR-101 with the IPv6oE Ethertype.

5.2 Access Node Forwarding Mechanisms

The requirements remain the same as in Section 3.2/TR-101.

5.3 QoS

R-03 The AN MUST support all the QoS requirements stated in Section 3.3/TR-101.

5.3.1 Traffic Classification and Class of Service Based Forwarding

R-04 The Access Node SHOULD support deriving the P-bit markings in the upstream direction based on an arbitrary combination of: user port, VLAN ID and received IPv6 Traffic Class value.

Note that the use of the Flow Label in the IPv6 Header is not considered for QoS.

5.4 IPv6 Interworking Functions

5.4.1 IPv6oE over ATM (U reference point)

The requirements for the IPv6oE interworking functions are defined in Section 5.6 and 5.7.

5.4.2 PPPoA

The requirements remain the same as in Section 3.5.4/TR-101.

5.5 L2 Security Considerations

This section provides security requirements for the Access Node. Many of these requirements are applicable to the N:1 VLAN configuration where user isolation is required, but several also apply in a 1:1 VLAN configuration. It should also be noted that some of the security features applicable for mass-market residential customers may not be applicable to some business customer configurations.

All Ethernet-related security aspects and requirements (MAC address spoofing, MAC address flooding, MAC-based filtering) remain as defined in TR-101.

5.6 Additional IWF for IPv6 over Ethernet based Access in N:1 VLANs

5.6.1 DHCPv6 Processing

R-05 The Access Node MUST be able to function as a Lightweight DHCPv6 Relay Agent (LDRA) according to draft-ietf-dhc-dhcpv6-ldra [24].

The requirement above is for IPv6 operation consistent with the architecture defined by TR-101 for IPv4, where the Access Node must be able to function as a Layer 2 DHCP Relay Agent (see Appendix B/TR-101). This is useful in order to allow the insertion of additional information that enables identification or characterization of the Access Loop.

Note that in the end-to-end network architecture, the BNG may act as a “full” DHCPv6 Relay Agent, providing additional DHCPv6 packet processing and insertion of additional information options that are of relevance to the BNG. The BNG will then send the packet to the DHCPv6 Server for further processing.

R-06 The Access Node MUST support enabling/disabling the LDRA function for all ports associated with specific S- TAGs.

The above requirement supports the N:1 VLAN scenario (in which case the LDRA will be enabled/disabled for all access ports associated with that VLAN) as well as the 1:1 VLAN scenario (in which case the LDRA will be enabled/disabled for one port only).

R-07 The Access Node MUST, when performing the function of an LDRA, be able to encode the access loop identification in the Interface-Id Option (option 18, defined in

RFC 3315 [14]) and add the option to the DHCPv6 Relay-forward messages sent to the BNG, which acts as a DHCPv6 server or a DHCPv6 Relay Agent.

R-08 When adding the Interface-Id, the encoding MUST uniquely identify the Access Node and the access loop logical port on the Access Node on which the DHCPv6 message was received. The Interface-Id contains a locally administered ASCII string generated by the Access Node, representing the corresponding access loop logical port (U interface). The actual syntax of the access loop identification in the Interface-Id is identical to the syntax defined in Section 3.9.3/TR-101 and Section 5.7/TR-156.

R-09 The Access Node MUST, when performing the function of an LDRA, be able to add the Relay Agent Remote-Id Option (option 37, defined in RFC 4649 [16]) to the DHCPv6 Relay-forward messages sent to the BNG, which acts as a Delegating Router and/or a DHCPv6 Relay Agent.

R-10 When adding the Relay Agent Remote-Id, the Access Node MUST set the remote-id field with a globally unique value that MUST be configurable by the Service Provider (for instance to uniquely identify the user on the associated access loop on the Access Node on which the DHCPv6 Solicit message was received). The actual syntax of the user identification in the Relay Agent Remote-Id is left unspecified in this Technical Report.

Note that in accordance with the DHCPv6 RFC 3315 [14] and draft-ietf-dhc-dhcpv6-ldra [24] the DHCPv6 Relay-Reply messages are unicast to the DHCPv6 client.

The Relay Agent Remote-Id option contains an enterprise-number field. The operator may choose to configure a value for the enterprise-number, or may decide to use a default value.

R-11 When adding the Relay Agent Remote-Id, the Access Node MUST set the enterprise-number field as follows:

- In the case where the operator did not provide the enterprise-number as part of the configuration of the Relay Agent Remote-Id option, the enterprise number MUST be set to the Broadband Forum enterprise code, i.e. 3561 in decimal (0x0DE9 in hexadecimal), corresponding to the IANA “ADSL Forum” entry in the Private Enterprise Numbers registry.
- In the case where the operator did provide the enterprise-number as part of the configuration of the Relay Agent Remote-Id option, the enterprise number MUST be set to the value provided by the operator.

RFC 3315 [14] defines the “Vendor-specific Information” Option (option 17). The option allows a (Lightweight) DHCPv6 Relay Agent to include vendor-specific data in the DHCPv6 messages it forwards as configured by the Service Provider. The use of this option is identical to the use of the DHCPv4 vendor-specific information option, and is detailed in TR-101 Appendix D - DHCP Vendor Specific Options to Support DSL Line Characteristics.

R-12 The Lightweight DHCP Relay Agent MUST support inserting the "Vendor-specific Information" Option (option 17) as per RFC 3315 [14] in order to add information about access loop characteristics. In this case, the enterprise-number MUST be set to

the Broadband Forum enterprise code, i.e. 3561 in decimal (0x0DE9 in hexadecimal), corresponding to the IANA "ADSL Forum" entry in the Private Enterprise Numbers registry. Access loop characteristics information is conveyed in the option-data field. In this field, the opt-code and the option-data subfields are specified in Table 3/TR-101.

5.6.2 Neighbor Discovery Processing

The default behavior for the Access Node is to forward all ICMPv6 messages. Table 1 summarizes the modification of this behavior with references to the corresponding requirements. Such behavior is recommended for residential subscribers.

In the table, the following terms are used:

- **Forward:** refers to the Access Node performing the normal forwarding rules (i.e. based on MAC destination address and/or VLAN ID)
- **Snoop:** refers to the Access Node inspecting (part of) the ICMPv6 message payload, deciding whether or not to discard the message, and optionally performing message manipulation before the message is forwarded according to the normal forwarding rules.
- **Discard**: refers to the Access Node discarding the message. It must be possible to disable this behavior (e.g. for business customers).

Table 1: ICMPv6 message processing

ICMPv6 type	Message name	Destination IP address	Upstream	Downstream
ICMPv6 error messages				
1	Destination Unreachable	Unicast	Forward	Forward
2	Packet Too Big	Unicast	Forward	Forward
3	Time Exceeded	Unicast	Forward	Forward
4	Parameter Problem	Unicast	Forward	Forward
ICMPv6 informational messages				
128	Echo Request	Unicast	Forward	Forward
129	Echo Reply	Unicast	Forward	Forward
Neighbor Discovery				
133	Router Solicitation	All-routers multicast	Snoop (R-15)	Discard (R-17)
134	Router Advertisement	Unicast to host sending RS	Discard (R-18)	Snoop (R-21)
		All-nodes multicast		
135	Neighbor Solicitation	Unicast of target	Forward	Forward
		Solicited-Node multicast address corresponding to the target		
136	Neighbor Advertisement	Unicast to host sending NS or All-nodes multicast	Forward	Forward

137	Redirect	unicast	Discard (R-19)	Forward

MLD				
130	Multicast Listener Query (MLDv1 & MLDv2)	*General Query*: link-scope all-nodes (ff02::1) *Multicast-Address-Specific Query*: multicast address being queried	Discard (R-20)	Forward

R-13 The AN MUST be configurable to either forward or discard unknown ICMPv6 messages.

R-14 The Access Node MUST support forwarding ICMPv6 packets destined to a multicast group.

5.6.2.1 Router Solicitation

In TR-101, the Access Node may add access line identification to DHCPv4 and/or PPPoE messages using a Layer 2 DHCPv4 Relay Agent or a PPPoE Intermediate Agent. A similar method exists in IPv6 using a Lightweight DHCPv6 Relay Agent, defined in Section 5.6.1. This is typically used in an N:1 VLAN deployment scenario.

When an RG or IPv6 host initializes its interface, it sends out a Router Solicitation (RS) message to obtain additional information from the BNG (e.g. the default router IPv6 address and/or the global prefix to be used for the WAN interface). In addition, the RG or IPv6 host may also send Neighbor Solicitation messages for the purpose of Duplicate Address Detection (DAD) to validate its link-local address.

Therefore, upon receiving the Router Solicitation message, the Access Node should be able to insert access line identification information in the RS message. This information can be used by the BNG to guide address assignment policies or enforce link-local address security. This mechanism would typically be used in an N:1 VLAN model.

R-15 The Access Node MUST be configurable to insert access line identification information in upstream Router Solicitation messages.

R-16 The Access Node SHOULD support R-15 according to draft-krishnan-6man-rs-mark [25].

The detailed problem statement, use cases and consequences of this function are described in Annex A.

Note: The corresponding Router Advertisement message from the BNG is a solicited multicast RA message using a L2 unicast according to R-44.

R-17 The Access Node SHOULD be configurable to discard RS messages received on a network interface.

5.6.2.2 Router Advertisement

R-18 The Access Node SHOULD be configurable to block upstream Router Advertisement messages originated by a host or RG.

5.6.2.3 Neighbor Solicitation

No specific actions are required by the Access Node, other than forwarding the packet.

NS messages are sent by the host/RG to resolve the BNG link-local address, and to perform Duplicate Address Detection.

NS messages are sent by the BNG to resolve the RG link-local address to a MAC address. Downstream NS messages may be sent to a specific host (unicast) or to the Solicited-Node multicast address associated with the Unicast address that needs to be resolved.

5.6.2.4 Neighbor Advertisement

No specific actions are required by the Access Node, other than forwarding the packet. Downstream NA messages may be sent to a specific host (unicast) or to all access lines (all-nodes multicast).

5.6.2.5 Redirect

R-19 The Access Node MUST be configurable to discard upstream Redirect messages originated by a host or RG.

5.6.2.6 Multicast Listener Query

R-20 The Access Node MUST be configurable to discard Multicast Listener Query messages received on a user interface.

5.6.2.7 Multicast Listener Report

According to RFC 4862 [13], “Before sending a Neighbor Solicitation, an interface MUST join the all-nodes multicast address and the solicited-node multicast address of the tentative address.” As a result, hosts will send MLD Multicast Listener Report messages for these multicast groups (ff02::1:ffXX:XXXX and ff01::1).

In order to ensure that subscriber connectivity is not impacted, these messages should be sent to the BNG unaltered. No specific processing is required on the Access Node.

5.6.3 IPv6 Spoofing Prevention

R-21 The Access Node SHOULD inspect upstream and downstream DHCPv6 messages (RFC 3315 [14], RFC 3633 [15]) and RA messages (RFC 4861 [12], RFC 4862 [13]) per user port and populate its IP Anti-spoofing Table accordingly, in order to prevent host IP address spoofing and delegated IP prefix spoofing.

R-22 Using the information obtained from R-21, the Access Node SHOULD provide a mechanism to prevent host IP address spoofing and delegated IP prefix spoofing.

R-23 The IP Anti-spoofing Table aging timers MUST be updated according to the liftetime information received from the Router Advertisement messages and DHCPv6 messages.

R-24 Dynamic entries in the IP Anti-spoofing Table MUST be aged out after the aging time.

5.7 Access Loop Identification and Characterization

The overall principles for access loop identification and characterization remain the same as those in TR-101.

5.7.1 Access Loop Identification Configuration and Syntax

The syntax requirements to encode the access loop identification in PPPoE, DHCP and DHCPv6 messages are the same as in Section 3.9.3/TR-101 and Section 5.7/TR-156.

5.7.2 Access Loop Characteristics

The encoding of Access Loop Characteristics in PPPoE, DHCP and DHCPv6 messages remain the same as in Section 3.9.4/TR-101. For DHCPv6, the encapsulation is defined in R-12.

5.7.3 Signaling the Access Loop Encapsulation

The signaling of Access Loop Encapsulation remains the same as in Section 3.9.5/TR-101.

5.7.4 BNG to RADIUS Signaling of Access Loop Characteristics

The signaling of Access Loop Characteristics in RADIUS messages remains the same as in Section 3.9.6/TR-101. Additional BNG requirements can be found in Section 6.2.

6 Broadband Network Gateway Requirements

6.1 IPv6 address assignment functions

As in the case of an IPv4 network, there are a number of different ways IPv6 addresses can be assigned to the WAN interface (e.g. DHCPv6 assigning a 128-bit address or SLAAC for assigning a /64 prefix) and how home network prefixes (e.g. /56) can be provided, namely:

- using an external DHCPv6 server
- using local IPv6 address pools configured on the BNG
- using a AAA server
- using Stateless Address Auto Configuration
- using static configuration

In the case where an external AAA/RADIUS Server is used for addresses assignment, the same RADIUS attributes (Framed-Interface-Id, Framed-IPv6-Prefix, Delegated-IPv6-Prefix, Framed-IPv6-Pool) and the same related BNG requirements specified in TR-187 are applicable for the equivalent purposes in the context of this Technical Report.

In an IPv4 BNG a single public address per customer has to be routed in the network, and being attached to the WAN interface of the CPE, this address is usually seen as directly reachable (one-hop) by the BNG. With IPv6 and when using a routed RG, a prefix is delegated to the RG (recommended prefix length: /56) and this prefix is used in the home LAN that is behind the RG. That means that this prefix is not directly reachable (one-hop) by the BNG. Instead, it is reachable via the RG (multi-hop). From the point of view of the BNG, the next hop for this prefix is:

- the RG's WAN link-local address (in the "unnumbered WAN" model)
- or the RG's WAN Globally-unique Unicast Address (in the "numbered WAN" model)

Compared to IPv4, an IPv6-enabled BNG therefore needs extra logic in order to be able to forward IPv6 datagrams to subscribers when the IPv6 destination belongs to a delegated prefix. This is achieved by letting the BNG retrieve the addressing information from the DHCPv6 messages in its internal DHCPv6 Relay Agent or DHCPv6 server, by processing these messages or by parsing the RAAN option [27]), if present. Then the BNG can automatically populate the addressing information in the IPv6 forwarding table.

This solution does not require the use of a routing protocol between the RG and the BNG. The information collected by the DHCPv6 Relay Agent or server of the BNG is directly and internally advertised to the routing instance located into the same node. No additional security functions are required.

Similarly, the DHCPv6 Relay Agent or DHCPv6 server notifies the routing instance that a route is no longer valid and must be removed when a DHCPv6 lease has expired or when a DHCPv6 Release message has been received (or relayed).

6.2 Routing table functions

R-25 When the BNG, acting as a DHCPv6 Relay Agent, receives a downstream Relay-Reply message containing a Reply message including an IA_PD option, it MUST add a route (allocated IPv6 prefix contained in the IA_PD, next hop contained in the peer-address field) to the relevant BNG routing table.

In the case of a routed RG, the peer-address field holds the link-local address of the WAN interface. In the case of a bridged RG, the peer-address field holds the link-local address of the IPv6 host behind the bridged RG.

R-26 When the DHCPv6 Relay Agent implemented in a BNG receives an upstream Release message (or a Relay-Forward message containing a Release message) including an IA_PD option, it MUST delete the route corresponding to the delegated prefix(es) indicated in this option.

R-27 When the lease related to a delegated prefix expires, the BNG MUST remove the corresponding route from the BNG routing table.

R-28 The BNG MUST be able to function as a Delegating Router.

R-29 When receiving an IA_PD option, the Delegating Router MUST NOT delegate the same prefix to any other RGs.

R-30 The BNG, when acting as a DHCPv6 Delegating Router or Server, MUST be able to use Option 18 in order to retrieve the Access Node identifier and access this table in order to identify the ad-hoc pool of prefixes or addresses.

R-31 When the DHCPv6 server implemented in a BNG sends a downstream DHCPv6 Reply message including an IA_PD option, it MUST add a route (allocated IPv6 prefix contained in the IA_PD, next hop contained in the destination address of the DHCPv6 Reply) to the relevant BNG routing table.

R-32 When the DHCPv6 server implemented in a BNG receives an upstream Release message (or a Relay-Forward message containing a Release message) including an IA_PD option, it MUST delete the route corresponding to the delegated prefix(es) indicated in this option.

R-33 The BNG MUST support sending the IPv6 AVP attributes in RADIUS messages, as defined in RFC 3162 [19] and in draft-ietf-radext-ipv6-access [28].

R-34 When a NAS implemented in a BNG receives a downstream RADIUS Access-Accept message sent by a RADIUS server that contains one or more Framed-IPv6-Route attribute (RFC 3162 [19]), it MUST add the corresponding routes to the relevant BNG routing table.

6.3 General

R-35 The BNG MUST support the unnumbered WAN model with IP sessions (DHCP).

R-36 When the BNG performs a RADIUS client function supporting both IPv4 and IPv6, it MUST assign IPv4 or/and IPv6 address and prefix to users as requested (RFC 3162 [19]).

6.4 QoS Hierarchical Scheduling

The requirements of Section 5.2/TR-101 apply without change.

R-37 The Broadband Network Gateway MUST be able to map between IPv4 or IPv6 traffic classes and the Ethernet priority field.

This requirement is the IPv6 augmentation of R-172/TR-101.

R-38 The Broadband Network Gateway, when receiving information about DSL synch rate parameters through PPP, DHCP or DHCPv6 (using the mechanism defined in R-12), MUST NOT apply the information in an additive fashion when multiple sessions are active on the same DSL line (the underlying synch rate is shared by all the sessions on a given DSL although each session will report the rate independently).

This requirement is the IPv6 augmentation of R-175/TR-101.

6.5 Neighbor Discovery Processing

R-39 The BNG MUST support sending RA messages with unique (per line) Prefix Information based on the access line identification information in the Router Solicitation message.

R-40 The BNG MUST support using the access line identification information in RS messages in order to determine what /64 prefix to advertise on an access line (the /64 prefix may be obtained by communicating to with a Radius server).

R-41 The BNG SHOULD support R-39 and R-40 according to the Line Identification Option (LIO) defined in draft-krishnan-6man-rs-mark [25].

The above requirements assumes that the Access Node has added access line identification information in the Router Solicitation messages. See also requirement R-15.

R-42 When sending a Prefix Information Option (PIO) in an RA message, the BNG MUST NOT advertise the same /64 prefix to different RGs / hosts on different access lines.

R-43 The BNG MUST be configurable to send multicast RA messages that do not contain a Prefix Information Option (PIO), in order to advertise the default router address.

R-44 The BNG SHOULD support sending periodic and solicited multicast RA messages having the unicast MAC address of the RG or of the hosts behind a bridged RG (see draft-gundavelli-v6ops-l2-unicast [26]).

R-45 The BNG must perform NS/NA message processing in accordance to RFC 4861 [12].

R-46 The BNG MUST support a mechanism to prevent more than one subscriber in a same broadcast domain from using the same link-local address. A possible mechanism is DAD-proxy as described in Annex B.

6.6 DHCPv6 Relay Agent

In the case of an IPv4 deployment, TR-101 specifies the BNG must support a DHCPv4 Relay Agent. In particular, the BNG must insert the gateway's IP address information in the giaddr field of the relayed message, in order to provide topological information to the DHCPv4 server. This giaddr information usually corresponds to the IPv4 address of the BNG's interface on which the client message was received. The giaddr information allows the DHCPv4 server to identify the pool (or a set of pools) of IPv4 addresses from which it chooses an IPv4 address to be allocated to the client.

In the case of an IPv6 deployment using prefix delegation, the same level of information needs to be transmitted to the DHCPv6 Delegating Router in order to identify the pool (or a set of pools) of IPv6 prefixes from which it chooses an IPv6 prefix to be delegated to the RG. A similar reasoning applies to DHCPv6 servers for the assignment of temporary and non-temporary IPv6 addresses, as per the corresponding Identity Associations.

Section 20.1.1 of RFC 3315 [14] specifies the following behavior:

If the relay agent received the message to be relayed from a client, the relay agent places a global or site-scoped address with a prefix assigned to the link on which the client should be assigned an address in the link-address field. This address will be used by the server to determine the link from which the client should be assigned an address and other configuration information.
[...] If the relay agent cannot use the address in the link-address field to identify the interface through which the response to the client will be relayed, the relay agent MUST include an Interface-id option [...] in the Relay-forward message.

In some deployments there is neither a need nor a desire to configure a global or unique local address to the interface on which the client messages are received. Such a deployment does not allow the BNG to insert an IPv6 address in the link-address field. Having the BNG insert an Interface-Id option (Optoin 18) allows identification of the interface on which the client messages are received, but it does not help the DHCPv6 Delegating Router or server to identify ad-hoc pools of prefixes or addresses.

In other deployments a globally unique or unique local address could be configured on the interface, but using a prefix that has no direct relationship with the prefixes to be assigned/delegated or the addresses to be assigned to the subscribers.

As introduced in this section, it can be deduced that the best solution for a DHCPv6 Delegating Router or Server to identify the pool of prefixes to be used for assignment consists of relying on the Interface-Id option (Optoin 18) inserted by the Access Node and more precisely on the Access Node identifier contained in this option.

The operator must maintain a table binding the Access Node identifier with the corresponding pool of prefixes. The DHCPv6 Delegating Router or DHCPv6 Server must be able to use Option 18 in order to retrieve the Access Node identifier and access this table in order to identify the ad-hoc pool of prefixes or addresses (see R-30).

The main advantage of this solution is that it does not bring any requirement to access or backhaul devices; additional functionality is only required on the DHCPv6 delegating router or server. Other solutions, such as relying on the Option 18 inserted by the BNG or the link-address field, are less generic.

R-47 The Broadband Network Gateway MUST be able to function as a DHCPv6 Relay Agent as described in RFC 3315 [14] on selected untrusted interfaces, i.e. when the Access Node is not acting as a Lightweight DHCPv6 Relay Agent.

R-48 The Broadband Network Gateway MUST be able to function as a DHCPv6 Relay Agent on selected trusted interfaces, i.e. when an Access Node acts as a Lightweight DHCPv6 Relay Agent according to draft-ietf-dhc-dhcpv6-ldra [24].

R-49 The Broadband Network Gateway MUST be able to disable the DHCPv6 Relay Agent on selected interfaces.

R-50 The Broadband Network Gateway MUST accept Relay-Forward messages with option 18 and option 37 received on its downstream interfaces (inserted by an Access Node acting as a Lightweight DHCPv6 Relay Agent according to draft-ietf-dhc-dhcpv6-ldra [24]).

R-51 The DHCPv6 Relay Agent of the BNG MUST be configurable to forward DHCPv6 messages to all the addresses on a provisioned list of DHCPv6 servers (including unicast addresses).

R-52 The BNG SHOULD support the DHCPv6 Bulk Leasequery mechanism as per RFC 5460 [17].

6.7 Security Functions

6.7.1 Source IPv6 Spoofing

R-53 When delegating the IPv6 prefix to a requesting router using RFC 3633 [15], the BNG MUST be able to populate the mapping of delegated prefix to MAC address in the IP Anti-spoofing table. by using the MAC address known by the BNG for the WAN interface of the RG.

R-54 The BNG when acting as DHCP Server MUST be able to inspect DHCPv6 (RFC 3315 [14]) per user, discover the mapping of IPv6 address to MAC address and populate its IP Anti-spoofing Table accordingly.

R-55 The DHCP Relay Agent in the BNG MUST be able to inspect DHCPv6 (RFC 3315 [14]) messages, discover the mapping of IPv6 addresses to MAC address and populate its IP Anti-spoofing Table accordingly.

R-56 The BNG MUST be able to populate its IP Anti-spoofing Table with prefixes that it has advertised in a Router Advertisement.

R-57 Having the knowledge of MAC to IPv6 mapping, the BNG MUST NOT send downstream multicast NS messages (similar to multicast ARP requests).

Note: R-57 should not be confused with the handling of downstream multicast RA messages having the unicast MAC address of the RG or of the hosts behind a bridged RG (see R-44).

7 Impact of IPv4 address exhaustion on IPv4 multicast

IPv4 multicast does not face the same address exhaustion problem as IPv4 unicast. As a result, it is expected that initial IPv6-based triple play deployments will maintain the current IPv4-based multicast network architecture.

Therefore, all requirements of TR-101 and TR-156 related to IPv4 multicast still apply in the TR-177 architecture.

In this model, the Set-Top Box continues to access IPv4 multicast content through the IPv4 group management protocol IGMPv2/v3. The RG and the access network also work according to the procedures specified in TR-101 and TR-124. To save IPv4 addresses, the IPv4 source address used by the IGMPv2/v3 proxy implemented in the RG, is the unspecified IPv4 address 0.0.0.0.

To make this possible, the following requirement needs to be met:

R-58 The Access Node MUST be able to accept and process upstream IGMPv2/v3 messages whose source address is 0.0.0.0 (unspecified address), irrespective of any IP anti-spoofing rules. This behaviour MUST be configurable per access line.

Note that according to TR-101 requirement R-235 and R-237, the RG must support sending IGMP messages having a source IPv4 address 0.0.0.0.

8 IPv6 Multicast

This version of the Technical Report does not describe the usage of IPv6 multicast requirements for the support of user plane multicast traffic such as it is used for IPTV.

Multicast functionalities are an integral part of the IPv6 specification and standardization performed by the IETF.

In particular, in IPv6, the Multicast Listener Discovery Protocol (MLD) is used by routers to discover the presence of multicast listeners (i.e., nodes that wish to receive multicast packets) on their directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes.

There are two versions of MLD available. Both versions are interoperable sub-protocols of ICMPv6 [6]. MLDv2 (RFC 3810 [21]), when compared to MLDv1 (RFC 2710 [20]), adds support for “source filtering”, as required to support Source-Specific Multicast.

As protocol for routing multicast traffic between routers Protocol Independent Multicast - Sparse Mode (PIM-SM) [23] is specified. PIM-SM is a multicast routing protocol that can use the underlying unicast routing information base or a separate multicast-capable routing information base. PIM-SM can be used for IPv4 and IPv6.

A description of specific IPv6 multicast requirements will be the subject of future BBF work.

9 Network Management

The requirements remain the same as in Section 8/TR-101. Management traffic can remain IPv4 based. This allows operators to keep the IPv4 network for management purposes and only introduce the IPv6 data and control planes for user traffic.

Annex A SLAAC in N:1 VLAN Topology

A.1 Introduction

Many of today's networks have different network domains and boundaries. Operators are facing the fact that certain partnering models in interconnection have to be realized e.g. because of regulatory reasons. Such a partnering model requires different access and aggregation domains to be connected to a common AAA architecture.

If for instance a 1:1 VLAN access domain and a different N:1 VLAN access domain are both connected to the same service provider and its AAA infrastructure, then the same mechanisms for IP address assignment, billing and accounting must be used in both access domains. In IPv6 based access networks this implies that the same IPv6 address and IPv6 prefix provisioning methods (and processes) have to be supported, e.g. for IPoE and PPPoE network models.

That leaves the choice regarding the selection of an appropriate address and prefix assignment model to the operators (ISPs and Telcos). Hence, in a 1:1 and N:1 VLAN topology, both a SLAAC-based as well as a DHCPv6-based provisioning method for the Globally-unique Unicast Address (GUA) of an RG have to be possible.

A.2 Illustration of a concrete Usage Scenario

A common usage scenario in today's broadband world is that service providers offer their services not only over their own access infrastructure but using also the network of other access providers. These service providers may face the challenge of having to use different VLAN models in the two network types. A typical use case is shown in the figure below, where service provider A uses in its access network a 1:1 VLAN model with a numbered WAN model and provides IPv6 address/prefix assignment via SLAAC/DHCPv6-PD. Provider A also offers the same service via a partner access network B (confederation network) using a N:1 VLAN model.

It would be advantageous for provider A is to use the same provisioning methods and processes for both network access scenarios.

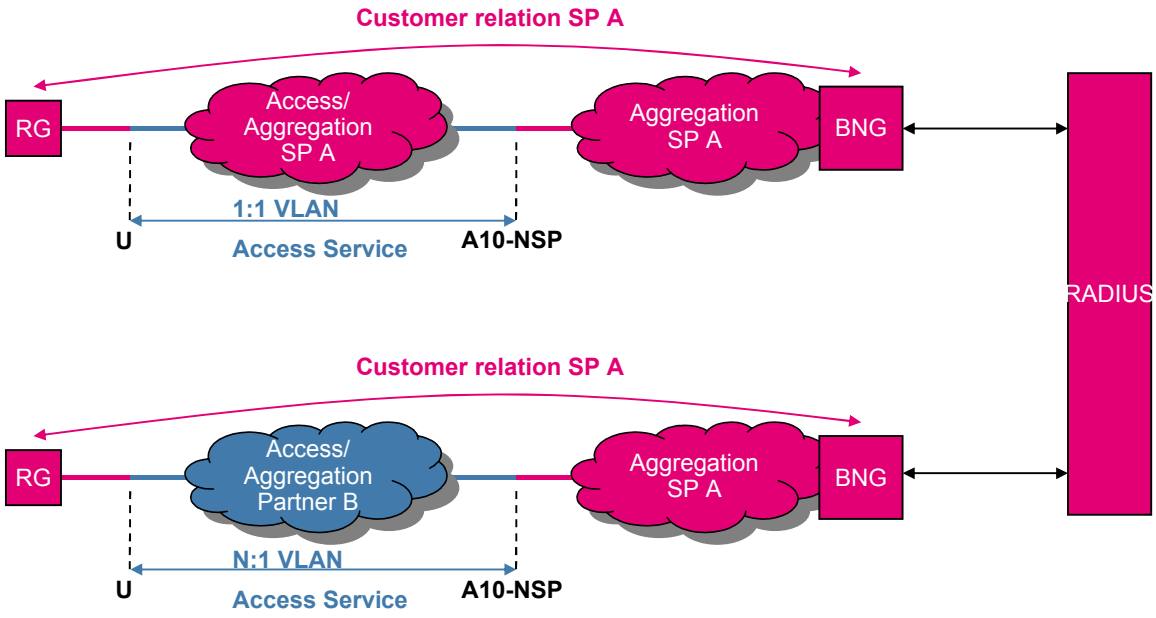

Figure 6 – Handoff architecture between IPv6 access provider and IPv6 service provider

A.3 Key building blocks and characteristics for using SLAAC in N:1 VLAN

The two key building blocks for the provisioning of a GUA to a WAN interface of an RG / host by using SLAAC in an N:1 VLAN scenario are:

1. Insertion of access Line Identification Option (LIO) in RS messages by the Access Node
2. Tunnelling of all RS and RA messages containing LIO between Access Node and BNG

The solution described in this annex meets the aforementioned requirement of using the same IPv6 address / prefix provisioning methods (and processes) for IPoE and PPPoE network models.

The following bullet points cover the detailed characteristics of this solution:

- Periodic IPv6 Multicast RAs are used for refreshing the Default Router and Prefix Information of all access lines. These multicast ICMPv6 messages are sent encapsulated towards the Access Node
- A Line Identification Option (LIO) is needed in tunneled RA messages in order to identify the corresponding access line where the RA message has to be forwarded to
- All RA messages containing LIOs have to be sent encapsulated towards the AN. These encapsulated messages are sent to the All-Node IPv6 MC Group address (according to RFC 4861 [12])

This approach has the benefit of resulting in a moderate load on AN and BNG and can also support SEND (SEcure Neighbor Discovery) if needed for any reasons.

A.4 Additional considerations

In general, SLAAC based IPv6 address configuration depends on the host sending an RS message to the BNG and then receiving an RA message from the BNG. A solution that requires the BNG to receive an RS message from the host and then sending an RA message back, is unreliable, since the RS message can be lost (e.g. on the DSL line, but in general on any network segment between the host and the BNG). To overcome this problem, the behavior of the RG needs to support a retransmission mechanism for RS messages.

The solution described in this annex can also be applied to hosts behind a bridged RG. In such a case however, the interface between the host and the bridged RG may be up before the access line is synchronized. This means the host will send RS messages without the BNG receiving them. As a result, the BNG won't send back an RA message to the host, and IPv6 connectivity is not achieved. Solutions for this specific case will be subject of future BBF work.

A.5 Basic message flow

In order to provide a better understanding of the SLAAC-based GUA provisioning solution for WAN interfaces in N:1 VLAN scenarios the below figure depicts the basic message flow:

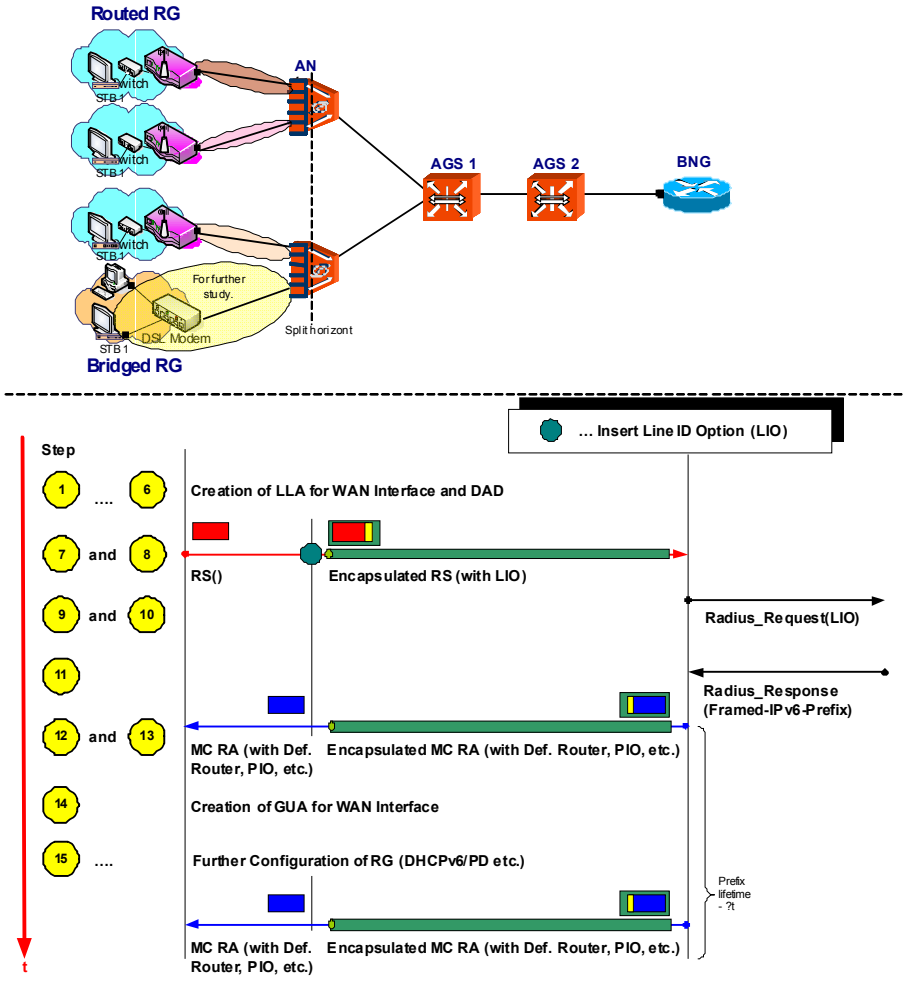

Figure 7 – Basic message flow for generation of the GUA of RG WAN interface

Initially a link-local IPv6 address is generated for the RG WAN interface. Network initialisation and Duplicate Address Detection is performed for this link-local address. A detailed description of these steps (1-6) is out of scope of this Annex.

In steps 7-12 the GUA generation of the WAN interface takes place as follows:

(7) The RG generates a Router Solicitation (RS) ICMPv6 message (Type 133, Code 0) with its link-local address as IPv6 source address (SA) and destination address (DA) ff02::2 („All link-local routers“-Multicast address). The MAC address of the RG is contained as „Source Link layer address“-Option.

(8) The Access Node encapsulates this RS message and inserts a Line Identification Option (LIO) into this encapsulated RS according to draft-krishnan-6man-rs-mark [25] and forwards it to the BNG.
(Note: this LIO will allow the BNG to identify the access line and to differentiate between the attached access lines and RGs).

(9) The BNG receives this encapsulated ICMPv6 message, de-capsulates it and checks on the basis of the LIO if it has already delegated a /64 for this access line.

(10) If it doesn't have such an entry, the BNG triggers Radius and requests a /64 for the Line ID of the access line.

(11) The BNG receives a response from the RADIUS server, including a Radius Framed-IPv6-Prefix Attribute containing a /64 prefix corresponding to the LIO.

(12) The BNG generates (according to RFC 4861 [12]) an IPv6 MC RA message to the ff02::1 "All link-local nodes" MC group. The BNG includes the /64 prefix of the access line in the Prefix Information Option (PIO) of the RA and sets the 'A'-flag of this PIO to 'True' in order to advise the RG or host to use the included PIO for the SLAAC of its WAN GUA. Besides that the 'Is-router' flag and the O-flags inside the RA are also set to 'True' in order to signal that the BNG is the Default Router and that more information can be provided by DHCPv6. This RA message is encapsulated in a newly created IPv6 datagram with the Line Identification Option (LIO) and is sent to the AN, according to draft-krishnan-6man-rs-mark [25]

(13) The AN receives this encapsulated RA message and if there is an LIO option present, the AN uses the line identification data of the LIO option to identify the access line on which the RA message should be forwarded. The AN removes the outer IPv6 header of this encapsulated / tunneled RA and multicasts the inner packet (the original RA) on this specific access line.

(14) The RG receives the RA and learns the Default Router and /64 IPv6 prefix for the access line. The RG generates a GUA for its WAN Interface from the /64 of the PIO and its Interface Identifier. The status for this GUA is set to 'Tentative'. DAD for this GUA is not needed since the RG itself is the only device that uses this /64 prefix. Hence the status of the GUA can be set to 'Valid' after sending a Neighbor Solicitation (NS) for the generated GUA and waiting for the corresponding Timeout.

Steps 15 and beyond perform the further configuration of the RG (if needed) by using for instance DHCPv6 or DHCPv6-PD in order to request additional information like DNS-Server address or an IPv6 Home LAN prefix (IA_PD).

Note 1: All periodic refreshes of the RA by the BNG as requested in RFC 4861 are also sent to IPv6 MC Address ff02::1 but tunneled to the AN according to draft-krishnan-6man-rs-mark [25]

The key benefit of the above solution is that no extra changes to the existing requirements of TR-124 are required and furthermore the fundamental architecture of TR-101 remains unchanged.

Annex B Duplicate Address Detection (DAD) Proxy

This annex describes a mechanism called DAD-proxy to solve the problem statement described in Section 4.8.1.2 concerning handling of duplicate link-local addresses in the N:1 VLAN scenario with split horizon. As described in that section, the proposed solution is based on the assumption that link-layer addresses on a VLAN are unique.

The main features of DAD-proxy are the following:
- It allows for a link-local address re-computation by an RG or a host whenever a link-local address is already in use
- It assists in building at the BNG a trusted <link-local address, link-layer address> mapping within a binding table
- If coupled with a filtering (antispoofing) function it prevents a spoofer from denying the service of a regular customer

Furthermore:
- It requires the support of a specific algorithm in the BNG to handle NS messages received from subscribers (in particular NS messages for DAD)
- It does not imply any change on the format of these messages
- It is compatible with RGs or hosts which do not use DAD or which are not able to change their link-local address in case of duplication. Naturally these devices cannot take benefit of the DAD-proxy, but an important point is that the existence of a DAD-proxy has no negative impact on them.

The DAD-proxy function is described in detail in draft-costa-6man-dad-proxy [29]. The following paragraphs remind the basic principles of this solution and explain how it can be used in the context of the architecture presented in this Technical Report.

B.1 DAD proxy in the BNG

If an RG or a host uses DAD[1], the BNG receives NS messages that these devices send on the WAN interface in order to check if a link-local address is already in use. In the text below these messages are called NS-DAD and the corresponding responses are called NA-DAD.

The BNG maintains a binding table per VLAN that maps link-local addresses to the respective MAC address of their owner. It is possible to limit the number of link-local addresses per MAC address (possibly, but not necessarily, to 1).

The BNG listens to all NS-DAD messages received from subscribers. When the BNG receives a NS-DAD from a subscriber on a VLAN, the BNG checks if the link-local address is already

[1] Duplicate Address Detection (defined in RFC 4862 [13]and RFC 4861 [12]). Note that DAD could be disabled in an RG or a host, but in this case it cannot benefit from the DAD proxy function in the IP edge.

known for the corresponding VLAN: in other words, it checks if the tentative link-local address is already present in the binding table mentioned above.

- If there is no existing entry related to the tentative link-local address, the BNG creates an entry in the binding table, by mapping the link-local address to the source MAC address of the NS-DAD.
- If an entry already exists and is bound to the same MAC address as the source MAC address of the NS-DAD, the BNG does nothing.
- If an entry already exists and is bound to another MAC address than the source MAC address of the NS-DAD, it means that probably another RG/host is already using the same link-local address. The BNG checks if the RG/host is still connected by sending out a unicast Neighbor Unreachability Detection (NUD) probe. If this check is successful, the address conflict is confirmed and then the BNG sends a unicast NA-DAD message to the RG/host that sent the NS-DAD.

According to RFC 4861 [12], NA-DAD messages have a multicast IPv6 destination. However, it is strongly recommended that the BNG send NA-DAD only to the requester for confidentiality purposes. Therefore, the BNG sends a NA-DAD message which has a multicast IPv6 destination address, but a unicast link-layer destination address on the Ethernet layer, as proposed by draft-gundavelli-v6ops-l2-unicast [26]. In particular the link-layer destination address is set to the link-layer source address of the corresponding NS-DAD. The source MAC address and the target link-layer address in the IPv6 payload are set to a BNG MAC address.

The DAD-proxy binding table can be maintained not only with the mechanism described above, but also with periodical or manually triggered NUD probes sent to test that the bindings are still in use.

B.2 Expected behavior of the BNG for hosts or RGs not supporting DAD

The binding table used by the DAD-proxy of the BNG must be filled not only when receiving a NS-DAD message, but also when receiving any packet whose source address is a link-local address. Otherwise the subscribers supporting DAD cannot be aware of the link-local addresses used by the subscribers not supporting DAD and the proposed solution becomes almost useless.

B.3 Coupling DAD-proxy with antispoofing in the BNG

In order to be useful, the DAD-proxy function must be coupled with an antispoofing function in the BNG. In other words, the DAD-proxy allows the subscribers to be aware that their address is a duplicate one and the antispoofing function prevents them from using a duplicate address. This is necessary to cover the security needs described in the problem statement of Section 4.8.1.2.

In order to do so, the BNG must discard a packet whose source IPv6 address is a link-local address if this address is known in the binding table for the corresponding VLAN, but bound to a different link-layer address.

B.4 Protection against flooding

This is useful to protect the BNG against malicious users that could try to overflow the link-local address binding table by sending a lot of messages with different link-local addresses.

B.5 Support by RG or host

The DAD-proxy solution is implemented in the BNG, but an RG or a host can benefit from DAD in order to change its link-local addresses on the WAN interface in case of conflict. In particular, if it receives a NA-DAD from the WAN interface, it means that link-local address is already in use by another subscriber. In this case it is recommended that the RG or the host generates a new link-local address[2] and restarts a new DAD phase. Otherwise, the auto configuration process is stopped and the WAN interface is either disabled or configured manually.

Note that, if an RG or a host does not use DAD (or the generation of a new link-local address in case of conflict), the BNG does not prevent it from accessing the service. Nevertheless, if a duplicate link-local address is detected, all the traffic coming from that RG or host with that link-local address is discarded. This is exactly what would happen also if the DAD-proxy function was not implemented in the BNG. In other words, the implementation of the DAD-proxy does not mandate any specific function in RGs or hosts: if they are not able to take advantage from DAD, their service is not made worse than without DAD-proxy.

B.6 Support by the Access Node or Aggregation Nodes

No function is needed in the Access Node or Aggregation Nodes in order to support the DAD-proxy solution described above.

End of Broadband Forum Technical Report TR-177

[2] The algorithm to generate a new link-local address is not described here. The new address could be a random address.

